

FILED

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA
(Alexandria Division)

2017 NOV 21 A 8:49

OVERSTOCK.COM, INC.,

Plaintiff,

v.

VIKTOR VISOCKY, *et al.*,

Defendants.

Civil Action No. 17-cv-1331

CLERK OF DISTRICT COURT
ALEXANDRIA, VIRGINIA

**BRIEF IN SUPPORT OF
PLAINTIFF'S *EX PARTE* MOTION
FOR TEMPORARY RESTRAINING
ORDER, ACCOUNT AND ASSET
FREEZE SEIZURE ORDER,
EXPEDITED DISCOVERY ORDER,
ORDER GRANTING ALTERNATIVE
SERVICE, AND ORDER TO SHOW
CAUSE RE: PRELIMINARY
INJUNCTION**

FILED UNDER SEAL

TABLE OF CONTENTS

PRELIMINARY STATEMENT	1
FACTUAL BACKGROUND	2
ARGUMENT	9
A. This Court Has Jurisdiction And Authority To Grant The <i>Ex Parte</i> Motion.....	9
B. This Court Should Grant The <i>Ex Parte</i> Motion, Because All Requirements Are Met	11
1. Overstock is Entitled to an <i>Ex Parte</i> TRO	11
2. Overstock Will Succeed On The Merits Of Its Claims	11
i. Lanham Act, 15 U.S.C. §§ 1114, 1125(a) - Defendants Counterfeited The Overstock	
Trademarks And Trade Dress	11
ii. CFAA, 18 U.S.C. § 1030(a)(5)(C) - Defendants' Phishing Scam Also Violates The	
Computer Fraud And Abuse Act	13
iii. Copyright Act, 17 U.S.C. §§ 101 <i>et seq.</i> - Defendants Also Infringed Overstock's	
Copyrighted Content.....	15
iv. Virginia Unfair Competition/Trademark Infringement - Defendants Also Violated	
Virginia Common Law	16
3. Overstock Has Suffered, And Will Continue To Suffer, Irreparable Harm	17
4. The Balance Of Hardships Tips Sharply In Overstock's Favor	18
5. The Public Should Be Free From Defendants' Phishing Scam	19
6. Only <i>Ex Parte</i> Relief Will Stop Defendants' Phishing Scam	20
i. Defendants Will Not Voluntarily Stop Phishing	20
ii. Notice Will Destroy The Court's Ability To Grant Effective Relief.....	20
iii. Defendants Will Move, Hide, Conceal, or Destroy Evidence	22
iv. <i>Ex Parte</i> Relief (Including a Seizure) Is Needed And Appropriate To Prevent	
Irreparable Harm.....	22
v. The Materials To Be Seized Are Located At The Seizure Locations.....	24
7. Overstock Needs Expedited Discovery	25
8. Overstock Needs Permission To Serve By Email And Other Electronic Means ..	27
CONCLUSION	31

TABLE OF AUTHORITIES

CASES

<i>AllscriptsMisys, LLC v. Am. Dig. Networks, LLC</i> , No. 1:10-cv-00111-MJG, 2010 U.S. Dist. LEXIS 4450 (D. Md. Jan. 22, 2010).....	21
<i>Application of U.S. of Am. for an Order Authorizing an In-Progress Trace of Wire Commc'ns over Tel. Facilities</i> , 616 F.2d 1122 (9th Cir. 1980)	26
<i>Arminius Schleifmittel GmbH v. Design Indus., Inc.</i> , 2007 U.S. Dist. LEXIS 10847 (M.D.N.C. 2007).....	17
<i>AT&T Broadband v. Tech Commc'ns, Inc.</i> , 381 F.3d 1309 (11th Cir. 2004)	22, 23
<i>Avvo Inc. v. Liang</i> , No. 2:16-cv-00892-DLR (D. Ariz. May 11, 2017)	passim
<i>Aztar Corp. v. MGM Casino</i> , No. 1:00-cv-00833-CMH, 2001 U.S. Dist. LEXIS 13118 (E.D. Va. Mar. 12, 2001).....	16
<i>Beckman Coulter, Inc. v. Beckcoulter.com</i> , No. 5:10-cv-03110-JF (N.D. Cal. July 26, 2010)	29
<i>Centro Tepeyac v. Montgomery Cty.</i> , 722 F.3d 188 (4th Cir. 2013)	11
<i>Chloe Sas v. Sawabeh Info. Servs. Co.</i> , No. 2:11-cv-04147-MMM-MAN, 2012 U.S. Dist. LEXIS 187818 (C.D. Cal. Dec. 5, 2012).....	23
<i>Craigslist Inc. v. 3Taps Inc.</i> , 942 F. Supp. 2d 962 (N.D. Cal. 2013)	14, 15
<i>Dell, Inc. v. Belgiumdomains.com, LLC</i> , 2007 U.S. Dist. LEXIS 98676 (S.D. Fla. Nov. 21, 2007)	21, 23
<i>Eurotech, Inc. v. Cosmos European Travels Aktiengesellschaft</i> , 213 F. Supp. 2d 612 (E.D. Va. 2002).....	17
<i>FMAC Loan Receivables v. Dagra</i> , 228 F.R.D. 531 (E.D. Va. 2005).....	28, 29
<i>Hard Drive Prods. v. Does 1-30</i> , 2011 U.S. Dist. LEXIS 73159, 2011 WL 2634166 (E.D. Va. Jul. 1, 2011).....	25, 27
<i>In re Baldwin-United Corp. (Single Premium Deferred Annuities Ins. Litig.)</i> , 770 F.2d 328 (2d Cir. 1985)	26
<i>In re Vuitton et Fils S.A.</i> , 606 F.2d 1 (2d Cir. 1979)	20, 23
<i>Kemp v. Peterson</i> , 940 F.2d 110 (4th Cir. 1991)	26
<i>Little Tor Auto Center v. Exxon Co. U.S.A.</i> , 822 F. Supp. 141, 143 (S.D.N.Y. 1993)	22
<i>Lone Star Steakhouse & Saloon, Inc. v. Alpha of Va., Inc.</i> , 43 F.3d 922 (4th Cir. 1995).....	16
<i>Malibu Media, LLC v. Doe</i> , No. 14-cv-03948-GLR, 2014 U.S. Dist. LEXIS 175283 (D. Md. Dec. 19, 2014)	25
<i>Microsoft Corp. v. John Does 1-18</i> , No. 1:13-cv-00139-LMB-TCB, 2014 U.S. Dist. LEXIS 48398 (E.D. Va. Jan. 6, 2014)	passim
<i>Microsoft Corp. v. John Does 1-2</i> , No. 1:16-cv-00993-GBL-TCB (E.D. Va. Aug. 22, 2017).....	passim
<i>Microsoft Corp. v. John Does 1-27</i> , No. 1:10-cv-00156-LMB-JFA (E.D. Va. Oct. 27, 2010)	15, 18, 21, 22
<i>Microsoft Corp. v. John Does 1-8</i> , No. 1:14-cv-00811-LO-IDD, 2015 U.S. Dist. LEXIS 110145 (E.D. Va. July 20, 2015).....	11
<i>Microsoft Corp. v. Jun Yan</i> , No. 3:10-cv-00162-VLB, 2010 U.S. Dist. LEXIS 14933 (D. Conn. Feb. 18, 2010)	23
<i>Mintel Learning Tech., Inc. v. Beijing Kaidi Educ. & Tech. Dev. Co.</i> , No. 4:06-cv-07541-PJH, 2007 U.S. Dist. LEXIS 103180 (N.D. Cal. Aug. 20, 2007).....	19
<i>Monoflo Int'l, Inc. v. Sahm</i> , 726 F. Supp. 121 (E.D. Va. 1989).....	16
<i>Mullane v. Cent. Hanover Bank & Tr. Co.</i> , 339 U.S. 306 (1950).....	28
<i>Mullane v. Central Hanover Bank & Tr. Co.</i> , 339 U.S. 306 (1950).....	28
<i>Multi-Channel TV Cable Co. v. Charlottesville Quality Cable Operating Co.</i> , 22 F.3d 546 (4th Cir. 1994)	17
<i>Otels, Inc. v. Metin Altun</i> , No. 1:11-cv-00604-AJT-JFA, 2012 U.S. Dist. LEXIS 114584 (E.D. Va. Aug. 14, 2012)	13
<i>Peri Hall & Assocs. v. Elliot Inst. for Soc. Scis. Research</i> , No. 4:06-cv-00202-GAF, 2006 U.S. Dist. LEXIS 26234 (W.D. Mo. Mar. 20, 2006).....	16
<i>Physicians Interactive v. Lathian Sys., Inc.</i> , 2003 U.S. Dist. LEXIS 22868 (E.D. Va. 2003)	19
<i>Precision Tune Auto Care v. Pinole Auto Care</i> , No. 1:00-cv-01748-GBL, 2001 U.S. Dist. LEXIS 24840 (E.D. Va. Oct. 15, 2001).....	16
<i>Ranco Indus. v. Bos. Floor Mats</i> , No. 4:10-cv-05214, 2011 U.S. Dist. LEXIS 38811 (S.D. Tex. Mar. 31, 2011).....	15
<i>Rio Props., Inc. v. Rio Int'l Interlink</i> , 284 F.3d 1007 (9th Cir. 2002).....	29
<i>SATA GmbH & Co. KG v. Wenzhou New Century Int'l</i> , No. 15-cv-08157-BRO-E, 2015 U.S. Dist. LEXIS 147637 (C.D. Cal. Oct. 19, 2015)	23
<i>Southwest Airlines Co. v. Farechase, Inc.</i> , 318 F. Supp. 2d 435 (N.D. Tex. 2004)	14
<i>United States v. New York Tel. Co.</i> , 434 U.S. 159 (1977)	26
<i>Venice Pl, LLC v. Does 1-12</i> , No. 5:17-cv-00333-BO, 2017 U.S. Dist. LEXIS 129581 (E.D.N.C. Aug. 15, 2017).....	25
<i>WhosHere, Inc. v. Orun</i> , No. 1:13-cv-00526-AJT, 2014 WL 670817 (E.D. Va. Feb. 20, 2014)	28

<i>Winter v. Nat. Res. Def. Council, Inc.</i> , 555 U.S. 7 (2008).....	11
--	----

STATUTES

15 U.S.C. § 1114(1)	12
15 U.S.C. § 1116(d)	23, 24
15 U.S.C. § 1125(a)	12
17 U.S.C. § 106	15
18 U.S.C. § 1030 (a)(5)(C)	14
18 U.S.C. § 1030(e)(2)(B)	14
28 U.S.C. § 1331	9
28 U.S.C. § 1367	10
28 U.S.C. § 1391(b)	10
All Writs Act, 28 U.S.C. § 1651(a)	25
Lanham Act, 15 U.S.C. § 1121.....	9

OTHER AUTHORITIES

4 C. Wright & A. Miller, <i>Federal Practice and Procedure</i> § 1061 (2d ed. 1987)	28
<i>Phishing</i> , FTC.gov, https://www.consumer.ftc.gov/articles/0003-phishing	4
<i>Scams and Safety Common Fraud Schemes Internet Fraud</i> , FBI.gov, https://www.fbi.gov/scams-and-safety/common-fraud-schemes/internet-fraud	4

RULES

Fed. R. Civ. P. 26(d)(1)	25
--------------------------------	----

PRELIMINARY STATEMENT

Defendants are cybercriminals running an Internet “phishing” scam from overseas. They identified popular U.S. shopping websites; created fully functioning copies of them (using a technique called “ripping”); and now, are using them to steal U.S. consumers’ credit card data.

Overstock and its customers are Defendants’ latest victims. Defendants targeted Overstock and its website, Overstock.com, because of their popularity and reputations. They also counterfeited the registered Overstock Trademarks on their fake shopping websites (the “Infringing Websites”), because Overstock.com uses the same marks throughout. Defendants count on consumer confusion—namely, confusion that the Infringing Websites are Overstock.com or associated with it. Defendants’ Websites ask for sensitive Shipping and Billing Information, which consumers provide because they trust Overstock with it. Then, Defendants appropriate that information to themselves—presumably, to use it or sell it to the highest bidder.

Overstock brings the instant lawsuit to stop Defendants’ phishing and permanently disable the Infringing Websites. Overstock brings the *Ex Parte* Motion to obtain Court orders to identify who Defendants really are (they are hiding their identities) and disable the Infringing Websites (and all associated domain name, web hosting, and payment processing accounts) during the pendency of the action and the busiest online shopping season of the year: the weeks leading up to Black Friday/Cyber Monday, and the December holidays.

As argued below, Overstock meets all requirements for emergency *ex parte* relief, namely: (1) a TRO, (2) an order to show cause re: preliminary injunction, (3) an account and asset freeze seizure order, (4) an order permitting alternative service, and (5) an order granting limited expedited discovery. Overstock must have these orders to protect itself and consumers; otherwise, Defendants will continue exploiting Overstock to defraud consumers.

FACTUAL BACKGROUND¹

1. Overstock and Overstock.com

Entrepreneurs founded Overstock in 1999; since then, it has grown from a small startup company into a billion-dollar retail giant. *See* Lee Decl. ¶ 4. Overstock's primary business is operating Overstock.com, a shopping website at the domain name <www.overstock.com>. *Id.* ¶¶ 36-37. Overstock always has owned and operated Overstock.com (the domain name and website). *Id.* ¶¶ 36-40. Because of Overstock's investments and success, it has become synonymous with Overstock.com, which, in turn, has become synonymous with safe, reliable shopping. *Id.* ¶ 15-17, 51-54.

2. The Overstock Trademarks And Other Protected Intellectual Property

Overstock owns several trademarks, which it prominently displays in the Overstock.com headers and navigation bars, and throughout the product listing and checkout pages. *Id.* ¶¶ 41-50. The "Overstock Trademarks" are defined as: OVERSTOCK (unregistered), OVERSTOCK.COM (U.S. Reg. No. 2,939,764), WORLDSTOCK (U.S. Reg. No. 2,945,081), WORLDSTOCK FAIR TRADE (U.S. Reg. No. 3,838,795), O (U.S. Reg. No. 3,265,584), O (Stylized) (U.S. Reg. No. 4,033,193), WE SAVE PEOPLE MONEY (U.S. Reg. No. 3,868,396), MAIN STREET REVOLUTION (U.S. Reg. No. 3,975,792), MAIN STREET (U.S. Reg. 4,053,685), and I LOVE LIVING (U.S. Reg. No. 4,847,333). All of these marks are registered or used for online wholesale/retail store services featuring general merchandise. *Id.* ¶¶ 41-48; *see also* Exhibit D thereto (USPTO Registration Certificates). Many of the marks have become legally famous and

¹The following facts come from the Declarations of Robert Holmes, Jr. ("Holmes Declaration" or "Holmes Decl."), Carter Lee ("Lee Declaration" or "Lee Decl."), and Marcella Ballard ("Ballard Declaration" or "Ballard Decl."), filed simultaneously herewith.

“incontestable.” *Id.* ¶ 45. Until now, all of the marks have been used exclusively and continuously by Overstock in connection with online shopping at Overstock.com.

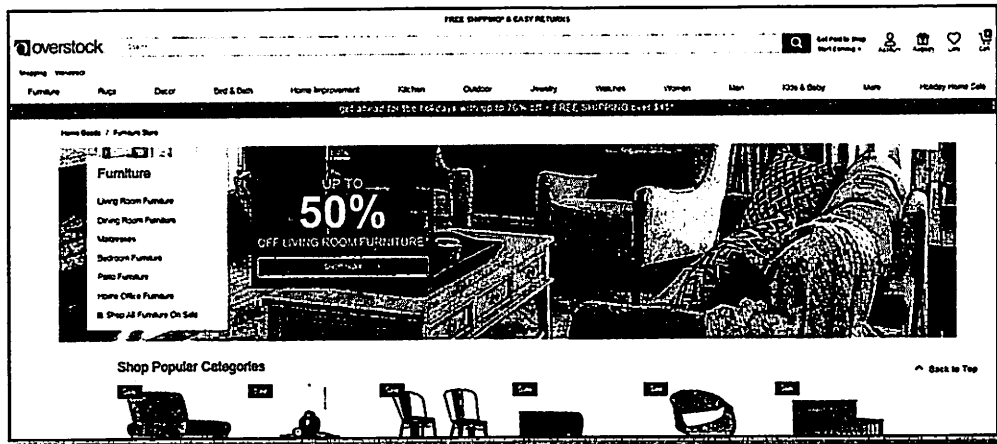
Overstock carefully chooses and uses its marks. It invests tremendous resources in branding and reputation-building, which can be as important as website functionality and security in online shopping. *Id.* ¶¶ 17-18, 53-54. Every time a consumer visits Overstock.com (or any other shopping website), they have a choice to make: Should I trust this website with my private data? This includes everything that is needed for an online storefront to process payment and complete an order: first name, last name, shipping address, billing address, phone number, email address, credit card number, credit card expiration date, and credit card security code. *See, e.g.,* Holmes Decl. ¶¶ 14, 17 (describing information needed to complete controlled buys *via* the Infringing Websites, described more fully below). Overstock gives its customers access to consistently safe online shopping. Lee Decl. ¶¶ 51-54. This causes customers to trust Overstock.com and to avoid asking each time whether it is trustworthy. *Id.* ¶ 53. Part of providing that consistency is Overstock.com’s consistent use of the Overstock Trademarks, and consistent designs and layouts of landing, product listing, and checkout pages. *Id.* ¶¶ 44, 48, 51-54. The website’s design, and its overall look-and-feel, is defined as the “Overstock Copyrighted Content” and “Overstock Trade Dress.” Both function as source identifiers, because of Overstock’s lengthy and consistent use of them. *Id.* ¶¶ 37, 44, 47-50.

3. Defendants’ Phishing Scam and Irreparable Harm

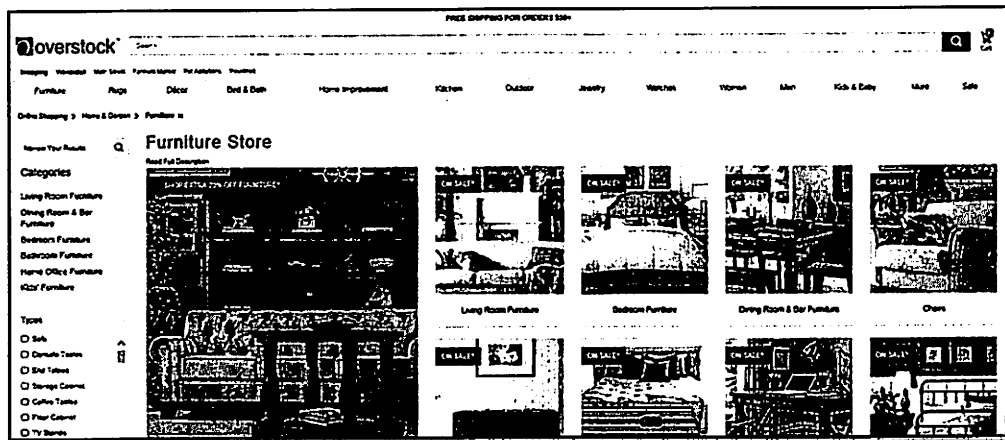
Defendants recognize the source-identifying capacity of the Overstock Trademarks, Copyrighted Content, and Trade Dress. They know that these assets are valuable. *Id.* ¶ 15. They know that consumers trust Overstock.com with contact information and credit card data. *Id.* ¶ 25-27. Because of this knowledge, they targeted Overstock and deliberately placed Overstock’s

source identifiers at the center of a “phishing scam.”² See Holmes Decl. ¶¶ 7-11, 477-78 (describing Defendants’ phishing scam and willfulness). As shown below, the Defendants’ “Infringing Websites” look just like Overstock.com—by design—because they must in order to work:

Overstock.com



Infringing Website – Highstockstore.com



4. Defendants’ Counterfeit, Infringing Websites

²The FBI defines phishing as a “virtual trap,” often involving fraudulent websites and emails. See *Scams and Safety | Common Fraud Schemes | Internet Fraud*, FBI.gov, <https://www.fbi.gov/scams-and-safety/common-fraud-schemes/internet-fraud>; see also *Phishing*, FTC.gov, <https://www.consumer.ftc.gov/articles/0003-phishing>.

The Infringing Websites are accessible via 17 .com domain names, all registered and located in the Eastern District of Virginia (where the .com domain name registry is located). *See* Holmes Decl. ¶ 13. Most of these domain names contain the term “STOCK,” creating an instant association with Overstock. *Id.* ¶ 7. Each was “ripped,” *i.e.*, copied full-cloth from the source code of Overstock.com. Holmes Decl. ¶¶ 18, 478. Because of this, each Infringing Website contains counterfeit copies of the Overstock Trademarks, Copyrighted Content, and Trade Dress. And, because of the sophisticated nature of the copying, consumers cannot distinguish between the Infringing Websites and Overstock.com. They mistakenly trust the Infringing Websites with their data, because they would trust Overstock with that data. Holmes Decl. ¶ 477. Defendants count on it.

4a. Overstock’s Controlled Buys

Overstock investigated and made a series of controlled buys from October 20 to 29, 2017. All buys followed the same steps. *See id.* ¶¶ 14-15. We include one example, which shows the nature of the scam at each Infringing Website:

Barneystock.com is an Infringing Website accessible at <www.barneystock.com>. Holmes Decl. ¶ 39. The first controlled buy occurred on October 20, 2017, when Overstock’s investigators accessed <www.barneystock.com> and were auto-redirected to <www.highstockstore.com>, which is another Infringing Website. Investigators noted the similarities between the Infringing Website and Overstock.com, namely, the Overstock Trademarks, Copyrighted Content, and Trade Dress, used in connection with purported online retail services. *Id.* ¶ 40. In fact, as set forth below, Defendants’ Infringing Websites sell no products. This is part of the scam.

At the Website, investigators saw hundreds of purported products, just like the products on Overstock.com. Investigators noted the lack of any Terms & Conditions, and the use of a fake contact address and phone number. *Id.* ¶ 41. Investigators chose a purported product to buy—“Pellon Decorative Pillow Insert” for \$7.95. *Id.* ¶ 42. Investigators went to the checkout page, where the Website displayed fillable forms requesting Shipping Information (*i.e.*, first name, last name, street address, city, state, zip code, phone number, and email address) and Billing Information (*i.e.*, billing contact first and last name, billing street address, billing city, billing state, billing zip code, billing phone number, email address, credit card number, credit card expiration date, and credit card security code). *Id.* ¶¶ 43-46. Investigators had an option to pay by non-traditional methods, such as PayPal, Bitcoin, or gift card, which are not offered on Overstock.com. *Id.* ¶ 45.

After entering Billing and Shipping Information, investigators clicked “Submit” to complete the purchase. *Id.* ¶ 47. The Website immediately displayed an error message common to phishing scams: “We are experiencing temporary technical difficulties and can’t accept Credit Card payment. Please select an alternate payment method. Please try using different credit card (Visa/Mastercard/Amex). Thank you for understanding.” *Id.* ¶ 48. In scams like these, messages like this give an excuse for why customers never receive the product. *Id.* ¶ 49. The message also provides an opportunity to phish for more data (*i.e.*, another credit card). If the consumer selects PayPal, Bitcoin, or giftcard, then the Website actually steals money in addition to the consumer’s data. *Id.* ¶ 60-61. Later, Defendants steal more money by repeatedly charging the credit card for increasing sums of money, until the customer notices and cancels the card.

Investigators also tried a second controlled buy on October 28, 2017. *Id.* ¶ 50. Again, investigators accessed <www.barneystock.com> from an IP address in the Eastern District of

Virginia. *Id.* ¶ 50. They immediately were redirected to an Infringing Website at <www.barneystockstore.com>. *Id.* They again saw all the Overstock source identifiers and fake contact information. *Id.* ¶ 51. They again tried to purchase the “Pellon Decorative Pillow Insert” for \$7.95. *Id.* ¶ 52. They again entered Shipping and Billing Information, and again received an error message: “Your card has been declined by our Merchant Gateway. Please try using different Credit card (Visa, Mastercard, Amex, Discover).” *Id.* ¶¶ 53-58. This time, investigators received a purported confirmation email from sales@barneystockstore.com, stating that an order was created (#70585) and could be completed by credit card, PayPal, Bitcoin, and a “wide range of alternate payment methods.” *Id.* ¶ 59. These error messages and emails also are common in phishing scams, but they are not common in authentic online retail. *Id.* ¶ 17-18. Investigators tried an “alternate payment method”: PayPal. *Id.* ¶ 60. They transferred funds to merchant arlankeen919604@yahoo.com, which is randomly generated and would not be the type of email address associated with a large online retailer. *Id.* ¶ 60. Sales@barneystockstore.com then sent another purported confirmation email, this time providing a purported tracking number, “US880836842US,” with a purported courier, “USN Carrier,” that does not exist. *Id.* ¶ 61-62. Defendants also “ripped” DHL’s website and uses it as the website for the fake USN Carrier. *Id.* ¶ 62.

No products were received. Shortly after completing the controlled buys, the credit card used to make the “purchases” was charged by unknown vendors, in increasing amounts, confirming identity theft. *Id.* ¶ 16. Investigators communicated with Overstock, and Overstock confirmed that Overstock.com was not accessed by any of the investigator’s IP addresses on the dates of the controlled buys (October 20 and 28, 2017). *Id.* ¶¶ 65-66. Overstock also examined the Infringing Websites and confirmed there is no affiliation with Overstock.com. Other the

investigator's reports, Overstock has no records of any attempts to make the controlled buys, which record would be generated automatically if the Infringing Websites were part of Overstock.com. *Id.* ¶¶ 65-66. This confirms that the Websites are counterfeit and so are the Overstock source identifiers that appear on them.

5. Defendants' Willfulness

Defendants' scam is willful. Defendants could not have ripped, copied, and republished spoofs of Overstock.com using 17 different domain names without active engagement and knowledge. Holmes Decl. ¶¶ 477-81. Phishing is illegal everywhere. Defendants know this and concealed their identities, so they would not get caught. For example, they use WHOIS privacy protection services for all 17 domain name registrations connected with the Infringing Websites, and the Websites display fake contact information to further Defendants' fraud. *Id.* ¶¶ 479-80. Defendants copied everything but Overstock.com's Terms & Conditions, demonstrating manual editing of the copied source code. *Id.* ¶¶ 18, 478. Similarly, Defendants removed some Overstock Trademarks from some of the pages, which shows that Defendants know they have no right to counterfeit these marks. Defendants also collected consumers' private data and in some cases money. *Id.* ¶ 7, 16, 482. They must know they have no right to the data or assets, and cannot possibly think their conduct is legal. Lee Decl. ¶¶ 31-35, 39-40, 59; Holmes Decl. ¶ 488. Thus, Defendants willfully created and are operating the Infringing Websites, and willfully counterfeited Overstock source identifiers. Holmes Decl. ¶¶ 477-85.

6. Harm to Overstock and Consumers

Phishing scams harm brand owners and consumers alike. Brand owners suffer harm to their reputations and trademark goodwill. Consumers suffer harm to their privacy interests—specifically, the right to share private data with who they want on their own terms. Here, Overstock and its customers are harmed because consumers have their data stolen and may learn not to trust

Overstock.com or the Overstock source identifiers. Some consumers may never use Overstock.com again, even if they know Overstock is not responsible for the Infringing Websites. The harm is magnified, now, entering into the busiest retail season of the year—the weeks leading up to Black Friday/Cyber Monday and the December Holidays. Unless this Court grants the *Ex Parte* Motion, Defendants’ phishing scam will continue, and Defendants will see the profits from their scam magnified as consumer purchasing increases between now and the end of December 2017.

ARGUMENT

To stop Defendants’ scam, Overstock needs *ex parte* relief in the form of: (1) a temporary restraining order (under Rule 65 and the Lanham Act, preventing further counterfeiting and phishing), (2) an account and asset freeze seizure order (under the Lanham Act, to shut down Defendants’ Infringing Websites and associated accounts, such as those used to create and operate domain names, host web content, and process payments), (3) expedited discovery (under Rule 26 and the All Writs Act, to find out who Defendants really are), (4) alternate service (under Rule 4, to quickly apprise Defendants and third parties of the action, because traditional service would be burdensome and futile), and (5) an order to show cause re: preliminary injunction (under Rule 65, to prevent further counterfeiting while this action is pending). The Court may grant this relief, and Overstock is entitled to it.

A. This Court Has Jurisdiction And Authority To Grant The *Ex Parte* Motion

Defendants’ scam violates numerous federal laws, namely, the Lanham Act, the Computer Fraud and Abuse Act, and the Copyright Act. Because of the violation of these statutes, the Court has original subject matter jurisdiction of Overstock’s claims under 28 U.S.C. §§ 1331, 1338. *See also* Lanham Act, 15 U.S.C. § 1121 (conferring original subject matter jurisdiction for Lanham

Act disputes). The Court also has ancillary jurisdiction over Overstock's Virginia law claims, because federal courts can hear "all other claims that are so related to claims in the action within such original jurisdiction that they form part of the same case or controversy." 28 U.S.C. § 1367. Here, Overstock's Virginia law claims have the same elements as the Lanham Act claims and require the same proof. The claims are inexorably related, and thus, the Court should consider them together.

The Court also has personal jurisdiction over Defendants, though they likely are outside the United States. *See* Holmes Decl. ¶ 13; Va. Code Ann. § 8.01-328.1(A)(1) (2017) (personal jurisdiction is proper where the Virginia court considers matters "related to the Defendant's business transactions" in the jurisdiction). Not only did all controlled buys occur in Virginia, but the Infringing Websites are targeted at Overstock's customers, many of whom reside in Virginia. Moreover, all 17 domain names are .com domain names, and the .com domain name registry VeriSign Inc. is located in this judicial district in Virginia. This makes the Court's exercise of jurisdiction reasonable. *See Microsoft Corp. v. John Does 1-18*, No. 1:13-cv-00139-LMB-TCB, 2014 U.S. Dist. LEXIS 48398, at *4 (E.D. Va. Jan. 6, 2014) (Brinkema, J.) (finding personal jurisdiction over non-U.S.-based cybercriminals, because they committed illegal acts through .com domain names located in this judicial district).

The proceeding also is properly venued. For venue to lay, a "substantial part" of the conduct or property at issue must be located in the jurisdiction, or, alternatively, where no other jurisdiction is appropriate, Defendants must be subject to personal jurisdiction. 28 U.S.C. § 1391(b). Here, both elements are met. The Defendants' .com domain names form a substantial part

of Defendants' phishing scheme, and they are physically located in Virginia with VeriSign Inc³. Defendants also are subject to personal jurisdiction, as discussed above. Thus, this Court has power and authority to hear the dispute and rule on the *Ex Parte* Motion.

B. This Court Should Grant The *Ex Parte* Motion, Because All Requirements Are Met

Overstock is entitled to the relief requested in the *Ex Parte* Motion. It satisfies all legal requirements and presents specific evidence proving that Defendants counterfeited the Overstock Trademarks, violated the Computer Fraud and Abuse Act, infringed Overstock's copyrights, etc. No other relief will provide an adequate remedy.

1. Overstock is Entitled to an *Ex Parte* TRO

A temporary restraining order is warranted if Overstock establishes, through evidence, that (1) it is likely to succeed on the merits of its claims; (2) it will suffer irreparable harm without the order; (3) the balance of the hardships tips in its favor; and (4) the order serves the public interest. *See Winter v. Nat. Res. Def. Council, Inc.*, 555 U.S. 7, 20 (2008); *Centro Tepeyac v. Montgomery Cty.*, 722 F.3d 184, 188 (4th Cir. 2013). Overstock's evidence establishes all four elements.

2. Overstock Will Succeed On The Merits Of Its Claims

Overstock will succeed on the merits of all of its claims in this proceeding.⁴

- i. Lanham Act, 15 U.S.C. §§ 1114, 1125(a) - Defendants Counterfeited The Overstock Trademarks And Trade Dress

³Other Eastern District of Virginia courts have drawn this conclusion. *See, e.g., Microsoft Corp. v. John Does 1-8*, No. 1:14-cv-00811-LO-IDD, 2015 U.S. Dist. LEXIS 110145, at *4 (E.D. Va. July 20, 2015); *Microsoft Corp. v. John Does 1-18*, No. 1:13-cv-00139-LMB-TCB, 2014 U.S. Dist. LEXIS 48398, at *4 (E.D. Va. Jan. 6, 2014) (Brinkema, J.).

⁴Overstock's Complaint sets forth federal and Virginia law claims for: (1) trademark infringement, in violation of Section 32 of the Lanham Act (15 U.S.C. § 1114); (2) violation of the Computer Fraud and Abuse Act (18 U.S.C. § 1030(a)(5)(C)); (3) copyright infringement, in violation of the Copyright Act of 1976 (17 U.S.C. §§ 101 *et seq.*); (4) false designation of origin, unfair competition, and trade dress infringement in violation of Section 43(a) of the Lanham Act (15 U.S.C. § 1125(a)); and (5) trademark infringement and unfair competition under Virginia common law.

The Lanham Act prohibits the reproduction, counterfeiting, copying, or production of a “colorable imitation” of a registered mark in connection with the distribution of goods and services, whenever there is a likelihood of confusion. To recover for trademark infringement under the Lanham Act, Overstock must show that it owns valid, protectable, trademarks; that Defendants used the marks in commerce without Overstock’s consent; and the unauthorized use resulted in likelihood of confusion. The same test applies in trade dress infringement cases. *See* 15 U.S.C. §§ 1114(1), 1125(a)⁵.

Undisputedly, Overstock owns the registered Overstock Trademarks. Overstock also owns the unregistered mark Overstock and the Overstock Trade Dress. These marks are valid, protectable, and, until now, exclusively used by Overstock.

Overstock also demonstrates through evidence (controlled buys) that Defendants used the registered Overstock Trademarks on the Infringing Websites, without permission. *See* Lee Decl. ¶¶ 57-59; Holmes Decl. ¶¶ 7-8, 10, 12, 15. Overstock’s evidence further demonstrates that Defendants’ use of the marks and the Overstock Trade Dress causes confusion—namely, confusion over whether Overstock operates the Infringing Websites. Thus, there is no question that Defendants’ infringed the registered and unregistered Overstock Trademarks and unregistered Trade Dress—and violated the Lanham Act.

Federal courts have drawn the same conclusion when presented with similar “phishing”

⁵*See also Thompson v. Haynes*, 305 F.3d 1369 (Fed. Cir. 2002) (holding that “[l]ikelihood of confusion ‘forms the gravamen’ for an action under [Section] 43(a) of the Lanham Act.”) (citation omitted); *Swatch, S.A. v. Beehive Wholesale, L.L.C.*, 888 F. Supp. 2d 738 (E.D. Va. 2012) (“In order to prevail on claims of trademark infringement and unfair competition under the Lanham Act, [. . .] a plaintiff must [] show ‘that the defendant’s use of a colorable imitation of the trademark is likely to cause confusion among consumers.’”) (citation omitted); *Beza Consulting, Inc. v. Yadeta*, No. 1:14-cv-00881-AJT-TCB, 2015 U.S. Dist. LEXIS 190147, at *7-8 (E.D. Va. May 11, 2015) (stating elements for trade dress infringement under federal law).

and computer fraud scenarios. *See, e.g., Microsoft Corp. v. John Does 1-2*, No. 1:16-cv-00993-GBL-TCB (E.D. Va. Aug. 22, 2017) (Lee, J.) (granting default judgment on Lanham Act claims where defendants used counterfeit versions of plaintiff's marks in websites and emails to deceive consumers into providing sensitive information or infecting their computers with a "bot" virus); *Avvo Inc. v. Liang*, No. 2:16-cv-00892-DLR (D. Ariz. May 11, 2017) (granting default judgment on Lanham Act claims where defendants created mirror websites using counterfeit versions of registered marks to trick consumers into disclosing personal information in a phishing scheme); *Microsoft Corp. v. John Does 1-18*, No. 13-cv-00139-LMB-TCB (E.D. Va. Apr. 3, 2014) (Brinkema, J.) (granting default judgment on Lanham Act claims where defendants created and distributed unauthorized copies of plaintiff's registered marks through websites bearing these counterfeit marks, deceiving consumers in the process); *Otels, Inc. v. Metin Altun*, No. 1:11-cv-00604-AJT-JFA, 2012 U.S. Dist. LEXIS 114584, at *12 (E.D. Va. Aug. 14, 2012) (Trenga, J.) (granting default judgment on Lanham Act claims where defendant used plaintiff's trademark in its domain name and throughout its website, where it used confusingly similar website layouts, and where its website was likely to confuse consumers into thinking it was affiliated with plaintiff). This Court should join those Courts in holding that Defendants' violated the Lanham Act, and it should find that Overstock has a likelihood of success on the merits of its Lanham Act claims.

ii. CFAA, 18 U.S.C. § 1030(a)(5)(C) - Defendants' Phishing Scam Also Violates The Computer Fraud And Abuse Act

The Computer Fraud and Abuse Act prohibits, among other things, intentionally accessing a protected computer without authorization, and as a result of such conduct, causing damage. 18

U.S.C. § 1030 (a)(5)(C). Under this framework a “protected computer” is one “which is used in or affecting interstate or foreign commerce or communication[.]” 18 U.S.C. § 1030(e)(2)(B).

Here, Overstock’s computers, which enable the shopping website Overstock.com, are “protected computers” under the CFAA.⁶ In “ripping” the entire content of Overstock.com, Defendants necessarily accessed these protected computers without permission.

Defendants’ unauthorized access to, and use of, Overstock’s computers and proprietary materials has caused significant harm to Overstock and consumers. Specifically, by creating the Infringing Websites to steal consumers’ data, Defendants are damaging and tarnishing the Overstock brand and Overstock’s reputation for safe, secure shopping. Defendants also deplete the consumer goodwill associated with the Overstock Trademarks and other source identifiers—which Overstock has worked painstakingly to develop. Moreover, Defendants’ behavior harms consumers directly, as the goal of Defendants’ scam is to collect and steal their data and their money, without providing goods or services in return.

This precise type of conduct is actionable under the CFAA. *See, e.g., Microsoft Corp. v. John Does 1-2*, No. 1:16-cv-00993-GBL-TCB (E.D. Va. Aug. 22, 2017) (Lee, J.) (finding a CFAA violation where defendants accessed Microsoft’s and consumers’ computers by reproducing and sending Microsoft trademarks and trade dress to consumers to trick them into downloading a “bot” virus); *Avvo Inc. v. Liang*, No. 2:16-cv-00892-DLR (D. Ariz. May 11, 2017) (finding a CFAA violation where defendants reproduced plaintiff’s entire website without authorization as a

⁶ “Protected computers” include computers “used in or affecting interstate or foreign commerce or communication.” 18 U.S.C. § 1030 (e)(2)(B). Courts have consistently recognized that corporate computers hosting website data are valid “protectable computers” under this provision. *See, e.g., Craigslist Inc. v. 3Taps Inc.*, 942 F. Supp. 2d 962 (N.D. Cal. 2013) (finding Plaintiff’s computers, hosting a commercial website in question, to be “protected computers” under the CFAA); *Southwest Airlines Co. v. Farechase, Inc.*, 318 F. Supp. 2d 435, 439-40 (N.D. Tex. 2004) (same).

phishing scheme to fool consumers into submitting sensitive information); *Craigslist Inc. v. 3Taps Inc.*, 942 F. Supp. 2d 962, 970 (N.D. Cal. 2013) (holding CFAA violated where defendant scraped proprietary data from plaintiff's website after plaintiff communicated a lack of authorization to do so); *Microsoft Corp. v. John Does 1-27*, No. 1:10-cv-00156-LMB-JFA (E.D. Va. Oct. 27, 2010) (Brinkema, J.) (finding a CFAA violation where defendants accessed Microsoft and consumer computers by reproducing plaintiff's trademarks and trade dress on websites and emails sent to trick consumers into downloading a virus). Given the evidence at hand, Overstock also will prevail its CFAA claim.

iii. Copyright Act, 17 U.S.C. §§ 101 *et seq.* - Defendants Also Infringed Overstock's Copyrighted Content

Under the Copyright Act, authors of original works fixed in a tangible medium possess exclusive rights, including the right to reproduce the work in question, to prepare derivative works, and to distribute copies of it. *See* 17 U.S.C. § 106. No other entities may engage in these activities, unless specifically authorized to do so, or unless the use is transformative fair use.

Here, Defendants copied the entire source code and content (*e.g.*, text, photographs, videos, layout and design) of Overstock.com—*a.k.a.*, the Overstock Copyrighted Content. The Defendants reproduced the Content—obviously, without Overstock's permission—on each Infringing Website. The purpose of the copying was not to “transform” the content, but to make the Infringing Websites look as close as possible to Overstock.com, so consumers would trust the Infringing Websites. This conduct plainly violates Overstock's copyrights in the Copyrighted Content. *See Avvo Inc. v. Liang*, No. 2:16-cv-00892-DLR (D. Ariz. May 11, 2017) (granting default judgment in favor of plaintiff's copyright claims where defendant copied plaintiff's copyrighted website layout, graphics, and text on a mirror phishing website); *accord Ranco Indus. v. Bos. Floor Mats*, No. 4:10-cv-05214, 2011 U.S. Dist. LEXIS 38811, at *8 (S.D. Tex. Mar. 31, 2011) (granting a

default judgment and permanent injunction where defendants “infringed [plaintiff’s] copyright by publishing a substantially similar website containing identical photographs and a substantially similar arrangement and text[.]”); *Peri Hall & Assocs. v. Elliot Inst. for Soc. Scis. Research*, No. 4:06-cv-00202-GAF, 2006 U.S. Dist. LEXIS 26234, at *4 (W.D. Mo. Mar. 20, 2006) (granting plaintiff’s request for a preliminary injunction where defendant created a website that “uses, mimics, and copies the look, feel, graphics, coding, and photos of the [plaintiff’s] website” and was created to confuse the public into believing the two websites were affiliated). Thus, Overstock is likely to succeed on the merits of its Copyright Act claim.

iv. Virginia Unfair Competition/Trademark Infringement - Defendants Also Violated Virginia Common Law

Virginia courts evaluate Virginia common-law trademark infringement and unfair competition claims under the same “likelihood of confusion” standard as equivalent Lanham Act claims. *See, e.g., Aztar Corp. v. MGM Casino*, No. 1:00-cv-00833-CMH, 2001 U.S. Dist. LEXIS 13118, at *14 (E.D. Va. Mar. 12, 2001) (citing *Lone Star Steakhouse & Saloon, Inc. v. Alpha of Va., Inc.*, 43 F.3d 922, 930 n.10 (4th Cir. 1995)) (“the test for trademark infringement and unfair competition under Virginia common law is essentially the same as that for trademark infringement under the Lanham Act because both address the likelihood of confusion as to the source of the goods or services involved”); *Precision Tune Auto Care v. Pinole Auto Care*, No. 1:00-cv-01748-GBL, 2001 U.S. Dist. LEXIS 24840, at *16-17 (E.D. Va. Oct. 15, 2001) (citing *Monoflo Int’l, Inc. v. Sahm*, 726 F. Supp. 121, 123 (E.D. Va. 1989)). Thus, Overstock has a likelihood of success on the merits of its Virginia law claims, because it has a likelihood of success on the merits of its Lanham Act claims, as argued above. *Accord Precision Tune Auto Care*, 2001 U.S. Dist. LEXIS 24840, at *16 (finding a likelihood of success on plaintiff’s common law claims where defendant used plaintiff’s trademarks on its building without authorization to confuse consumers into

believing they would receive good or services from plaintiff); *Eurotech, Inc. v. Cosmos European Travels Aktiengesellschaft*, 213 F. Supp. 2d 612, 623, 627 (E.D. Va. 2002) (Ellis, J.) (finding a likelihood of success on Plaintiff's Lanham Act unfair competition and trademark infringement claims, and thus its common law claims for the same).

3. Overstock Has Suffered, And Will Continue To Suffer, Irreparable Harm

Overstock cannot stop Defendants' scam without *ex parte* relief. If Overstock does not get relief, it and its consumers will suffer continued irreparable harm. Specifically, Overstock will suffer harm to its reputation as a trusted online wholesaler and retailer. It will continue to lose investments in the Overstock Trademarks, Copyrighted Content, and Trade Dress. Consumers will continue to be tricked, lured into a false sense of security, and have their data stolen. None of this harm is compensable with money, because once consumer trust is eroded, it may never come back. Likewise, once data is stolen, it cannot be recalled. *See Multi-Channel TV Cable Co. v. Charlottesville Quality Cable Operating Co.*, 22 F.3d 546, 552 (4th Cir. 1994), *abrogated on other grounds by Winter v. Nat. Res. Def. Council, Inc.*, 555 U.S. 7 (2008)) (holding that "when the failing to grant preliminary relief creates the possibility of permanent loss of customers to a competitor or the loss of goodwill, the irreparable injury prong is satisfied. . . ."); *Arminius Schleifmittel GmbH v. Design Indus., Inc.*, 2007 U.S. Dist. LEXIS 10847, at *22 (M.D.N.C. 2007) (finding irreparable harm because defendant's conduct "will have significant and continuous long-term effects."). Courts faced with similar circumstances have consistently held that this harm constitutes "immediate and irreparable injury, loss, or damage." *See, e.g., Microsoft Corp. v. John Does 1-2*, No. 1:16-cv-00993-GBL-TCB (E.D. Va. Aug. 22, 2017) (Lee, J.); *Avvo Inc. v. Liang*, No. 2:16-cv-00892-DLR (D. Ariz. May 11, 2017) (granting *ex parte* temporary restraining order and preliminary injunction, where, as here, the defendant created a mirror website using

counterfeits plaintiff's marks to defraud consumers in a phishing scheme); *Microsoft Corp. v. John Does 1-18*, No. 1:13-cv-00139-LMB-TCB (E.D. Va. Apr. 3, 2014) (Brinkema, J.) (same, where defendants used plaintiff's marks to deceive consumers into disclosing private information to malicious "bot" software); *Microsoft Corp. v. John Does 1-27*, No. 1:10-cv-00156-LMB-JFA (E.D. Va. Oct. 27, 2010) (Brinkema, J.).

4. The Balance Of Hardships Tips Sharply In Overstock's Favor

Overstock and consumers have suffered great harm, but the Defendants will not suffer any harm to any legally protected interest if the Court grants the *Ex Parte* Motion. The imposition of an injunction or freeze on Defendants' accounts will not harm Defendants in any legally cognizable way, as the sole purpose of the accounts associated with the Infringing Websites is to carry out illegal activity. Under similar circumstances, Courts consistently find that the balance of hardship tips against defendants. *See Avvo Inc. v. Liang*, No. 2:16-cv-00892-DLR (D. Ariz. May 11, 2017) (granting an *ex parte* TRO and noting that the balance of hardships weighed in plaintiff's favor where "issuance of the [TRO] would merely stop Defendants [. . .] from displaying their copy of Plaintiff's website, which contains Plaintiff's intellectual property, and failure to issue the [TRO] would cause Plaintiff to suffer irreparable injury to its intellectual property and reputation and would permit Defendant [. . .] to continue using the Website to steal the personal information Internet users believing they were on Plaintiff's website[.]"); *Microsoft Corp. v. John Does 1-18*, No. 1:13-cv-00139-LMB-TCB (E.D. Va. Apr. 3, 2014) (Brinkema, J.) (granting *ex parte* TRO and seizure order where granting the orders would only prevent unlawful conduct and denying the orders would result in further irreparable harm to plaintiff and its customers).

Also, to the extent the *Ex Parte* Motion affects third parties like domain name registrars, registries, web hosts, privacy protection services, search engines, and banks or other financial

institutions, the inconvenience will be minimal and temporary. Overstock narrowly tailored its Proposed Order and simply requests that these parties take defined actions to freeze Defendants' accounts to dismantle the Infringing Websites. Any burden is warranted, because the third parties' help is critical to stopping Defendants' counterfeiting and phishing scam.

5. The Public Should Be Free From Defendants' Phishing Scam

Defendants have no right to counterfeit Overstock's Trademarks or steal consumers' information, whereas consumers have a right to be free from Defendants' phishing scam. Even looking beyond Overstock and its customers, the public must remain free of risks posed by Internet phishing, and that risk is present while Defendants' Infringing Websites remain online. Granting the *Ex Parte* Motion will protect the public, whereas denying it will hurt the public by leaving them vulnerable to phishing. This is precisely the type of scenario in which courts have held that the public interest is served by immediate *ex parte* injunctive relief. *See, e.g., Intel Learning Tech., Inc. v. Beijing Kaidi Educ. & Tech. Dev. Co.*, No. 4:06-cv-07541-PJH, 2007 U.S. Dist. LEXIS 103180, at *29-30 (N.D. Cal. Aug. 20, 2007) (noting that each jurisdiction "has a significant interest in protecting the intellectual property of its citizens and businesses from infringement by foreign defendants."); *Physicians Interactive v. Lathian Sys., Inc.*, 2003 U.S. Dist. LEXIS 22868, at *30 (E.D. Va. 2003) (granting a TRO and preliminary injunction request where the defendant hacked into a computer and stole information, noting that "[t]his court has an obligation to enjoin any computer hackers from continuing to attack and steal [plaintiff's] proprietary information."); *Avvo Inc. v. Liang*, No. 2:16-cv-00892-DLR (D. Ariz. May 11, 2017) (holding that, where defendants ripped Plaintiff's intellectual property to trick consumers into disclosing personal information on identical phishing websites, the "[i]ssuance of a restraining order is in the public interest, and there is no likelihood of harm to the public from the issuance of

the restraining order.”).

6. Only *Ex Parte* Relief Will Stop Defendants’ Phishing Scam

i. Defendants Will Not Voluntarily Stop Phishing

Defendants know that what they are doing is illegal, and that knowledge has not stopped them. Therefore, it is reasonable to assume Defendants will not stop phishing just because Overstock asks them to, or because Overstock filed a lawsuit under U.S. law. Defendants, who may not be located in the United States, deliberately structured their scam to stay outside of any U.S. court’s reach (so they thought), by concealing their identities and using multiple layers of anonymity and subterfuge. Something must stop Defendants from counterfeiting and phishing, and the *Ex Parte* Motion is the only means to do it.

ii. Notice Will Destroy The Court’s Ability To Grant Effective Relief

If Defendants have notice of this proceeding before the Court rules on the *Ex Parte* Motion, then they will immediately take further steps to avoid responsibility, .e.g., by moving the content at the Infringing Websites to different domain names (perhaps .net or .org domain names that are not “present” in Virginia), or by moving to different web hosts, IP addresses, or domain name servers. The movement will not undercut Defendants’ ability to deceive and defraud consumers—it will only change the location at which the deception and fraud occurs. If Defendants move the content, Overstock would have no ability to stop their conduct in this proceeding, and the investigation and enforcement of Defendants would have to start anew.

Courts in this and other jurisdictions have held that *ex parte* relief is warranted in this particular circumstance, *i.e.*, where notice to opposing parties would render the requested relief futile. *In re Vuitton et Fils S.A.*, 606 F.2d 1 (2d Cir. 1979) (holding notice prior to issuing a TRO was inappropriate where it would only “serve to render fruitless further prosecution of the action”

based on prior experience that once one member of a counterfeiting operation received notice of a proceeding against it, contraband would be transferred or concealed); *AllscriptsMisys, LLC v. Am. Dig. Networks, LLC*, No. 1:10-cv-00111-MJG, 2010 U.S. Dist. LEXIS 4450, at *2 (D. Md. Jan. 22, 2010) (granting an *ex parte* TRO where “defendant may dissipate the funds and/or take action to render it difficult to recover funds. . . .”). Operators of similar websites have long been known to evade enforcement attempts by moving their domain names, IP addresses, and servers. *Avvo Inc. v. Liang*, No. 2:16-cv-00892-DLR (D. Ariz. May 11, 2017) (granting *ex parte* TRO and recognizing the risk that Defendants in internet phishing scheme would relocate to avoid prosecution)⁷; *Dell, Inc. v. Belgiumdomains.com, LLC*, 2007 U.S. Dist. LEXIS 98676, at *4-5 (S.D. Fla. Nov. 21, 2007). Similarly, in no less than three different cases heard by this court involving defendants using counterfeit trademarks and infringing trade dress online to trick consumers into disclosing information or downloading viruses, the court has found that defendants were likely to move or conceal their operations if given advanced notice of the proceeding. *Microsoft Corp. v. John Does 1-2*, No. 1:16-cv-00993-GBL-TCB (E.D. Va. Aug. 22, 2017) (Lee, J.) (granting plaintiff’s request for alternative service, including through e-mail, where defendants were likely international entities and had already endeavored to hide their identities using privacy protection services); *Microsoft Corp. v. John Does 1-18*, No. 1:13-cv-00139-LMB-TCB (E.D. Va. Apr. 3, 2014) (Brinkema, J.) (same); *Microsoft Corp. v. John Does 1-27*, No. 1:10-cv-00156-LMB-JFA (E.D. Va. Oct. 27, 2010) (Brinkema, J.). This Court should make the same findings here.

⁷In *Avvo*, when granting plaintiff’s request for an *ex parte* TRO against defendants’ operating websites using counterfeit plaintiff trademarks and trade dress to trick consumers into disclosing sensitive data the court noted that *ex parte* relief was appropriate in part because it was apparent that “Defendants [. . .] migrate the counterfeit website from domain to domain, seeking to evade efforts to target the site to suppress its phishing scheme.” *Avvo*, No. 2:16-cv-00892-DLR (D. Ariz. Apr. 4, 2016) (Order granting TRO).

iii. Defendants Will Move, Hide, Conceal, or Destroy Evidence

In addition to moving operations, Defendants will conceal or destroy relevant evidence if given advance notice. Courts faced with similar circumstances have consistently recognized this reality and have issued emergency *ex parte* relief. See *AT&T Broadband v. Tech Commc'ns, Inc.*, 381 F.3d 1309, 1319-20 (11th Cir. 2004) (affirming *ex parte* search and seizure order to seize contraband technical equipment given evidence that Defendants and other similar entities had concealed and moved evidence after notice was given); *Microsoft Corp. v. John Does 1-2*, 1:16-cv-993 (E.D. Va. Aug. 22, 2017) (Lee, J.) (approving *ex parte* TRO because there was “good cause” to believe Defendants operating a “bot” scheme using Plaintiff’s trademarks would move or destroy evidence upon notice of the case); *Avvo Inc. v. Liang*, No. 2:16-cv-00892-DLR (D. Ariz. May 11, 2017) (approving *ex parte* TRO where there was good cause to believe that Defendants operating an online phishing scheme used Plaintiff’s trademarks would move or destroy evidence upon notice of adverse proceedings); *Microsoft Corp. v. John Does 1-18*, No. 1:13-cv-00139-LMB-TCB (E.D. Va. Apr. 3, 2014) (Brinkema, J.) (approving *ex parte* TRO because there was “good cause” to believe Defendants operating a “bot” scheme using Plaintiff’s trademarks would move or destroy evidence upon notice of the case); *Microsoft Corp. v. John Does 1-27*, No. 1:10-cv-00156-LMB-JFA (E.D. Va. Oct. 27, 2010) (Brinkema, J.) (same); *Little Tor Auto Center v. Exxon Co. U.S.A.*, 822 F. Supp. 141, 143 (S.D.N.Y. 1993) (*ex parte* TRO approved where it was shown that contraband “may be destroyed as soon as notice is given.”). As such, *ex parte* relief is warranted here.

iv. *Ex Parte* Relief (Including a Seizure) Is Needed And Appropriate To Prevent Irreparable Harm

Section 1116(d) of the Lanham Act provides for the *ex parte* seizure of instrumentalities used to produce counterfeits, as well as materials involved in making and using counterfeit marks,

and records related thereto. 15 U.S.C. § 1116(d). Records includes hard-copy records, as well as electronically stored information residing on servers, computers, and other electronic devices. *See, e.g., Microsoft Corp. v. Jun Yan*, No. 3:10-cv-00162-VLB, 2010 U.S. Dist. LEXIS 14933, at *1 (D. Conn. Feb. 18, 2010) (granting TRO and temporary order impounding products); *AT&T Broadband*, 381 F.3d 1309, 1319 (11th Cir. 2004) (approving an *ex parte* TRO and seizure order allowing the seizure of, among other things, “all correspondence with customers, sales invoices, purchase orders, return forms, receipts, bank records, safe deposit box records, proceeds of sales, insurance policies, safes, shipping labels and tax returns of other business records, including all computer terminals, hard drives, servers, disks, and tapes in their possession . . .”); *In re Vuitton et Fils S.A.*, 606 F.2d at 4; *SATA GmbH & Co. KG v. Wenzhou New Century Int’l*, No. 15-cv-08157-BRO-E, 2015 U.S. Dist. LEXIS 147637, at *35 (C.D. Cal. Oct. 19, 2015) (approving an *ex parte* TRO and seizure order allowing the seizure of, among other things “computer disks, CD ROMs, computer hardware, laptops, computers, PDAs, cellphones, and other magnetically or electronically stored information.”); *Chloe Sas v. Sawabeh Info. Servs. Co.*, No. 2:11-cv-04147-MMM-MAN, 2012 U.S. Dist. LEXIS 187818, at *8 (C.D. Cal. Dec. 5, 2012) (affirming the validity of an *ex parte* seizure order allowing the seizure of, among other things, the servers for counterfeit websites); *Dell, Inc.*, 2007 U.S. Dist. LEXIS 98676 at *4-5 (approving an *ex parte* TRO and seizure order allowing for a forensic analysis of defendants’ computer data for records).

Overstock’s *Ex Parte* Motion seeking a seizure is legally appropriate, because it will prevent irreparable harm, it is narrowly tailored, and: (1) no order other than an *ex parte* seizure is adequate to prevent further counterfeiting (*see* discussion, *supra*, pp. 20-22); (2) Overstock has not publicized the requested seizure (*see* Lee Decl. ¶¶ 74-75); (3) Overstock will succeed in showing that Defendants used counterfeit marks in connection with the Infringing Websites (*see*

discussion, *supra*, pp. 11-17); (4) Overstock will suffer irreparable harm (*see* discussion, *supra*, pp. 17-18); (5) the matter to be seized will be located at the place identified in the application (*see* discussion, *infra*, pp. 24-25); (6) the balance of hardships tips in Overstock's favor (*see* discussion, *supra*, pp. 18-19); and (7) Defendants would readily destroy, move, or hide the instrumentalities of the counterfeiting and phishing scheme, and all associated records (including records showing their true identities) (*see* discussion, *supra*, pp. 20-22; 15 U.S.C. § 1116(d)(4)(B)(i)-(vii) (setting forth the statutory prerequisites for obtaining an *ex parte* seizure); *see also* Ballard Decl. ¶¶ 7, 13-15 (confirming that all statutory requirements are met in this case, and attaching the letter to the U.S. Attorney).

The need for *ex parte* seizure is demonstrated clearly by *Avvo Inc. v. Chang Liang*. In *Avvo*, the court granted an *ex parte* seizure order because of the likelihood that defendants, running a phishing scheme through infringing websites mirroring Plaintiff Avvo's website, would move, conceal, or destroy evidence if give notice of the proceeding. No. 2:16-cv-00892-DLR (D. Ariz. May 11, 2017). Similarly, in *Microsoft Corp. v. John Does 1-2*, the court granted an *ex parte* seizure order because of the likelihood that defendants would delete or relocate their malicious software, allowing them to continue to directly harm plaintiff's customers. No. 1:16-cv-00993-GBL-TCB (E.D. Va. Aug. 5, 2016) (Lee, J.). This *ex parte* seizure order is plainly warranted, both to preserve relevant evidence and to effectively halt Defendants' phishing scam involving the Overstock Trademarks.

v. Materials To Be Seized Are Located At The Seizure Locations

Evidence will be found with third-party service providers whose services are used as instrumentalities of Defendants' phishing scheme, namely, Defendants' accounts with domain name registries, domain name registrars, web hosts, WHOIS privacy protection services, payment

processors, back-end service providers, web designers, sponsored search engine or ad word providers, and banks and merchant account providers used by the Defendants. The evidence consists of information about Defendants, their concealed identities, their victims, and their victims' damages. Defendants have used these third parties to create, maintain, and operate the Infringing Websites and to perpetuate their phishing scam. Thus, information related to the scam will be found within the accounts.

7. Overstock Needs Expedited Discovery

Overstock also requests limited, expedited discovery from the third parties, with discovery targeted to learning Defendants' true identities and addresses, and confirming the locations and instrumentalities of their unlawful operations. Under Federal Rule of Civil Procedure 26, parties may commence discovery before the Rule 26(f) conference if authorized by court order. Fed. R. Civ. P. 26(d)(1). Within this Circuit, district courts have found good cause for expedited discovery when, among other things, the true identities of the defendants are unknown, the moving party alleges infringement, the scope of the discovery sought is narrow, and expedited discovery would substantially contribute to moving the case forward. *See, e.g., Venice PI, LLC v. Does 1-12*, No. 5:17-cv-00333-BO, 2017 U.S. Dist. LEXIS 129581, at *2 (E.D.N.C. Aug. 15, 2017); *Malibu Media, LLC v. Doe*, No. 14-cv-03948-GLR, 2014 U.S. Dist. LEXIS 175283, at *1 (D. Md. Dec. 19, 2014). Courts also granted expedited discovery where plaintiffs established irreparable harm, and where plaintiffs are unable to discover defendants' identities except through third-party discovery, such as discovery served on internet service providers. *See, e.g., Hard Drive Prods. v. Does 1-30*, 2011 U.S. Dist. LEXIS 73159, 2011 WL 2634166 (E.D. Va. Jul. 1, 2011).

Separately, under the All Writs Act, 28 U.S.C. § 1651(a), the court may issue all writs necessary or appropriate for the administration of justice. This provision repeatedly is invoked to

direct third parties to take narrowly-defined actions to implement court orders. *United States v. New York Tel. Co.*, 434 U.S. 159, 179 (1977) (All Writs Act authorized granting an order to a telephone company directing it to assist in the implementation of a pen registrar warrant); *Kemp v. Peterson*, 940 F.2d 110, 113 (4th Cir. 1991) (affirming the District Court's authority under the All Writs Act to order a monthly accounting because "the order bears a direct relationship to the district court's purpose of monitoring compliance with the freeze order."); *In re Baldwin-United Corp. (Single Premium Deferred Annuities Ins. Litig.)*, 770 F.2d 328, 338 (2d Cir. 1985) ("An important feature of the All-Writs Act is its grant of authority to enjoin and bind non-parties to an action when needed to preserve the court's ability to reach or enforce its decision in a case over which it has proper jurisdiction."); *Application of U.S. of Am. for an Order Authorizing an In-Progress Trace of Wire Commc'ns over Tel. Facilities*, 616 F.2d 1122, 1129 (9th Cir. 1980) (upholding an order requiring a third party to provide specific information to the plaintiff; noting that in *New York Tel. Co.* "the Court made the commonsense observation that, without the participation of the telephone company, 'there is no conceivable way in which the surveillance authorized could have been successfully accomplished.'") (citations omitted). Thus, the All Writs Act provides separate authority for granting expedited discovery.

Here, Overstock establishes a strong need and good cause for ordering expedited discovery. As set forth above, Defendants took great care to hide their identities to further the counterfeiting and phishing schemes. So far, Overstock has only identified Defendants by their domain names and publicly available information from their domain name registrars and web hosts. However, the use of privacy protection services and fake addresses means Overstock does not know who Defendants really are. The third-party service providers do know, however, and could easily share that information with Overstock. Overstock's requested expedited discovery is extremely limited

to: (1) the names and addresses of the Defendants and the locations of their operations, including identifying information associated with Defendants' websites, and any other domain names, merchant accounts, and payment accounts they may operate; (2) any and all known Internet websites on which Defendants use the Overstock Trademarks, Trade Dress, or Copyrighted Content; (3) any and all known domain names registered by Defendants; and (4) any and all financial accounts owned or controlled by Defendants. Granting Overstock's request for expedited discovery will allow it to more fully identify Defendants and will substantially further this litigation by ensuring that the correct individuals receive proper service of process, reducing the likelihood of time-consuming motion practice related to incorrect identification of defendants. *See, e.g., Hard Drive Prods. v. Does 1-30*, 2011 U.S. Dist. LEXIS 73159, 2011 WL 2634166, at *2-4 (E.D. Va. Jul. 1, 2011). Moreover, granting expedited discovery will permit Overstock and third parties to fully and properly execute the relief afforded by the *Ex Parte* Motion (should the Court grant it). Thus, Overstock's request for limited expedited discovery is reasonable, and supported by the law and good cause.

8. Overstock Needs Permission To Serve By Email And Other Electronic Means

Overstock also needs permission to deviate from Rule 4 and serve Defendants/third parties by alternative means. Overstock submits that good cause exists for alternative service, because Defendants intentionally use the Internet to operate anonymously, to avoid detection and prevent service or enforcement of others' rights, all the while conducting an unlawful scam that harms Overstock and the public. Defendants' efforts to conceal their identities makes it impossible for Plaintiffs to know, at this early stage, whether the names and addresses associated with their domain names are accurate, or whether other individuals are also operating these accounts. Additionally, the only addresses available for traditional service are the fake addresses displayed

on the Infringing Websites. Service at those addresses would be futile, because Overstock's investigation shows that Defendants are not located there—nor could they be, because other business are located there and/or the locations could not support a purported retail operation of the Infringing Websites' apparent size.

The goal of Rule 4 is to provide flexibility in the procedures for giving defendants notice of an action and to eliminate unnecessary technicalities in the service of process. 4 C. Wright & A. Miller, *Federal Practice and Procedure* § 1061, at 216 (2d ed. 1987). Due process requires that service be “reasonably calculated, under all circumstances, to appraise interested parties of the pendency of the action and afford them an opportunity to present their objections.” *Mullane v. Central Hanover Bank & Tr. Co.*, 339 U.S. 306, 314 (1950). Thus, both the Federal Rules of Civil Procedure and the U.S. Supreme Court have recognized service by mail, facsimile, email and publication as valid methods of providing notice to foreign, anonymous defendants in certain circumstances.

Courts also have recognized that service by mail, facsimile, email, and publication satisfies Due Process in instances where it is reasonably calculated to notify parties of a TRO, seizure order, preliminary injunction hearing, and complaint. *WhosHere, Inc. v. Orun*, No. 1:13-cv-00526-AJT, 2014 WL 670817, at *3 (E.D. Va. Feb. 20, 2014) (citing *Mullane v. Cent. Hanover Bank & Tr. Co.*, 339 U.S. 306 (1950)) (finding service via e-mail and social media accounts comports with Due Process where defendant provided such e-mail addresses and was responsive on such social media accounts); *FMAC Loan Receivables v. Dagra*, 228 F.R.D. 531, 535 (E.D. Va. 2005) (acknowledging that courts “around the country” have consistently allowed alternative forms of service, including service by e-mail, facsimile, mail, and publication). Here, Defendants' counterfeiting and phishing occurs online, entirely through Internet-based mechanisms. It only

makes sense that Defendants should be served *via* online, Internet-based methods, which are the methods they have chosen to accomplish their scheme.

Alternative service is particularly appropriate here, because Defendants endeavored to hide their location and true identities, and are shown to have done business online, and to have caused irreparable damage through web-based misconduct. *See Rio Props., Inc. v. Rio Int'l Interlink*, 284 F.3d 1007, 1014-15, 1018 (9th Cir. 2002) (noting that “when faced with an international e-business scofflaw, playing hide-and-seek with the federal court, email may be the only means of effecting service of process.”); *Beckman Coulter, Inc. v. Beckcoults.com*, No. 5:10-cv-03110-JF (N.D. Cal. July 26, 2010) (granting TRO where international defendants operated an e-mail phishing scheme and a website exactly identical to plaintiff’s, confusing and harming consumers); *FMAC Loan Receivables*, 228 F.R.D. at 536 (E.D. Va. 2005). Here again, Defendants are anonymous entities known to have committed fraudulent acts *via* the internet. Though they have actively worked to conceal their identities and locations through domain registrar privacy protection services, they were obligated to provide a legitimate email address to their domain registrars to register their websites. Thus, email addresses obtained from these registrars are likely to be the most reliable form of contact with, and service on, Defendants. Defendants also may expect service of process at these addresses, as they likely agreed to service at these addresses in their contract with domain registrars. Thus, notice and service by mail, facsimile, e-mail and publication are not only appropriate, but necessary, in this instance.

Plaintiff also respectfully requests permission to serve the relevant Orders upon necessary third parties by the same alternative means. Time is of the essence to ensure that Defendants do not move, destroy, or otherwise conceal assets and evidence connected with their unlawful activities, which may be accessible through their various accounts. Overstock must be able to serve

any Order and related papers upon the appropriate third-party service providers as quickly as possible. Service by electronic means and/or by overnight courier are the most effective means of notifying necessary third parties of the Order. Additionally, these service methods can be tracked, monitored, and confirmed upon delivery.

In an abundance of caution, if the Court sees fit to grant Overstock's *Ex Parte* Motion, Overstock also will personally serve the registered agents of all third parties. Service to these parties is critical to the effectiveness of the requested relief, because, as described above, it is likely that they are the only parties that possess reliable information about Defendants' true identities and contact information.

Overstock Will Provide Notice To Defendants By Personal Delivery: Under the requested Order, Overstock will endeavor to obtain physical addresses for Defendants from domain registrars and hosting companies, then will plan to effect formal service by hand delivery at these addresses.

Overstock Will Provide Notice By Email, Facsimile, And Mail: Overstock has identified a number of e-mail addresses and/or facsimile numbers for Defendants, and certain domain name registrar "abuse contact" e-mail addresses. In addition to these addresses, Overstock plans to obtain further e-mail and/or facsimile information from Defendants' domain registrars or web hosts under the requested Order, and will use those to effect service.

Overstock Will Provide Notice To Defendants By Publication: Overstock will provide Defendants notice of the instant proceeding by publishing case materials on a publicly accessible, centrally located Internet source for six months.

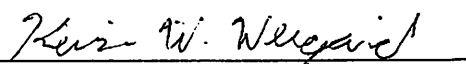
The foregoing methods of providing notice to Defendants satisfy Due Process and are appropriate and reasonable means to provide notice in this instance. As such, this Court should approve and order the alternative means of service listed above.

CONCLUSION

For the foregoing reasons, Overstock respectfully requests that this court grant its *Ex Parte* Motion, in its entirety, and further requests that this Court order other, further relief deemed just or proper.

Dated: November 21, 2017

VENABLE LLP


Randall K. Miller (VSB 70672)
Nicholas M. DePalma (VSB No. 72886)
Kevin W. Weigand (VSB No. 81073)
8010 Towers Crescent Drive, Ste 300
Tysons Corner, VA 22182
(703) 905-1449 (Tel)
(703) 821-8949 (Fax)
rkmill@venable.com

Marcella Ballard (Pro Hac Vice Pending)
1270 Avenue of the Americas, 25th Floor
New York, NY 10020
Tel.: 212-307-5500
Fax: 212-307-5598
MBallard@Venable.com

Counsel for Plaintiff Overstock.com, Inc.